EV436703072

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No. .....
Filing Date ..... Filed Concurrently Herewith
Inventorship ..... Mironov
Applicant ..... Microsoft Corporation
Attorney's Docket No. MS1-1921US
Title: Stream Cipher Design with Revolving Buffers

INFORMATION DISCLOSURE STATEMENT

References -- See Attached Form PTO-1449

REMARKS

The citations listed, copies of non- patent references attached, are submitted in compliance with the duty of disclosure defined in 37 CFR §1.56. The Examiner is requested to make these citations of official record in this application.

Respectfully Submitted,

Date: March 31, 2004

By: Ramin Aghevli
Ramin Aghevli
Reg. No. 43,462

Please type a plus sign (+) inside this box → [+]

EV439703072

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Mironov
Group Art Unit	
Examiner Name	
Attorney Docket Number	MS1-1921US

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		6,496,928		Deo et al.	12-17-2002	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Office[3]	Number[4]	Kind Code[5] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Please type a plus sign (+) inside this box → [+]

EV430703072

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	
Filing Date	
First Named Inventor	Mironov
Group Art Unit	
Examiner Name	
Attorney Docket Number	MS1-1921US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		ALON, N., ROICHMAN, Y.; "Random Cayley Graphs and Expanders" RSA: Random Structures & Algorithms; January 7, 1997; 15 pgs	
		COURTOIS, N.; "Algebraic Attacks on Combiners with Memory and Several Outputs" Published on the internet at http://eprint.iacr.org/2003/125/. Presented at Crypto 2003, 17 pgs	
		GOLIC, J. Dj.; "Cryptanalysis of Alleged A5 Stream Cipher" Springer-Verlag, 1998, pgs 239-255	
		HALEVI, S., COPPERSMITH, D., JUTLA, C.; "Scream: a software-efficient stream cipher" Published on the internet at http://eprint.iacr.org/2002/019.pdf. June 2002, pgs 1-21	
		ROGAWAY, P., COPPERSMITH, D.; "A Software-Optimized Encryption Algorithm" Journal of Cryptology: the journal of the International Association for Cryptologic Research, 1994, Revised Sept. 1997, 16 pgs	
		MENEZES, A., van OORSCHOT, P., VANSTONE, S.; "Handbook of Applied Crypotography" CRC Press, 1996 / 1997; Chapter 1 "Overview of Crytography" pgs 1-48	
		MENEZES, A., van OORSCHOT, P., VANSTONE, S.; "Handbook of Applied Crypotography" CRC Press, 1996 / 1997; Chapter 6 "Stream Ciphers" pgs 191-222	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.